arXiv:math/0512269v1 [math.NT] 13 Dec 2005

AN IMPROVEMENT OF A LARGE SIEVE INEQUALITY IN HIGH DIMENSIONS

LIANGYI ZHAO

Abstract. In this paper, we present an improvement of a large sieve type inequality in high dimensions and discuss its implications on a related problem.

1. Introduction

It was in 1941 that J. V. Linnik [11] first introduced the idea of large sieve in the investigation of the distribution of quadratic non-residues. Applications of the idea abound.

The large sieve inequality, the present form of which was first introduced by H. Davenport and H. Halberstam [4], is stated as follows. There are many references on the subject. See, for example, [1, 2, 5, 12, 13]. We shall henceforth refer to it as the classical large sieve inequality. For notational convenience, a set of real numbers $\{x_k\}$ is said to be δ-spaced modulo 1 if $\|x_j - x_k\| > \delta$, for all $j \neq k$, where henceforth if $x = (x_1, \cdots, x_n) \in \mathbb{R}^n$ $\|x\|$ denotes $\max\limits_i \min\limits_{k\in\mathbb{Z}} |x_i - k|$.

Theorem 1 (Classical Large Sieve Ineqaulity)**.** *Let $\{a_n\}$ be an arbitrary set of complex numbers, $\{x_k\}$ be a set of real numbers that is δ-spaced modulo 1, and $M \in \mathbb{Z}$, $N \in \mathbb{N}$. Then*

$$\sum_k \left| \sum_{n=M+1}^{M+N} a_n e(x_k n) \right|^2 \ll (\delta^{-1} + N) \sum_{n=M+1}^{M+N} |a_n|^2, \tag{1.1}$$

where the implied constant is absolute.

Save for the more precise implied constant, the above inequality is the best possible. Montgomery and Vaughan [14] showed that

$$\sum_k \left| \sum_{n=M+1}^{M+N} a_n e\left(x_k n\right) \right|^2 \leq \left(\delta^{-1} + N\right) \sum_{n=M+1}^{M+N} |a_n|^2, \tag{1.2}$$

while Paul Cohen and Selberg have shown independently that $\delta^{-1} + N$ can be replaced by $\delta^{-1} + N - 1$ which is absolutely the best possible, since Bombieri and Davenport [3] gave examples of $\{x_k\}$ and a_n, with $\delta \to 0$, $N \to \infty$ and $N\delta \to \infty$ such that equality holds in (1.2) with $\delta^{-1} + N - 1$. However, in our paper, we shall not be concerned with the implied constants.

As corollaries to Theorem 1, we have the following inequality for additive characters.

$$\sum_{q=1}^{Q} \sum_{\substack{a \bmod q \\ \gcd(a,q)=1}} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q} n\right) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2. \tag{1.3}$$

Various extensions of these classical results restricted to various kinds of special characters are also known [16, 17]. Results similar to (1.1) are also known in higher dimension and the proof is also similar. The following is quoted from [8].

Date: February 2, 2008.

Theorem 2. *Let*

$$S(x_1,\cdots,x_k)=\sum_{n_1,\cdots,n_k} c(n_1,\cdots,n_k)e(n_1x_1+\cdots+n_kx_k),$$

where the summation is over integer points in k dimensional rectangle. $M_j<n_j\le M_j+N_j$ for $j=1,\cdots,k$. Let $x^{(1)},\cdots,x^{(R)}$ be real k dimensional vectors, say $x^{(r)}=(x_1^{(r)},\cdots,x_k^{(r)})$, which satisfy

$$\max_j \delta_j^{-1}\|x_j^{(r)}-x_j^{(s)}\|>1,$$

for all $r\neq s$, where δ_j's are positive numbers not exceeding $\frac{1}{2}$. Then we have

$$\sum_{r=1}^{R}\left|S(x^{(r)})\right|^2\le\prod_{j=1}^{k}\left(\sqrt{N_j}+\sqrt{\delta_j^{-1}}\right)^2\sum_{n_1,\cdots,n_k}|c(n_1,\cdots,n_k)|^2. \tag{1.4}$$

Note that the length of the outer summation on the left-hand side of (1.1) does not exceed δ^{-1} and analogous statements can be made about that of (1.4), and that the right-hand sides of (1.1), (1.3) and (1.4) are essentially the sum of the lengths of the summations on the left-hand sides times the square of the l_2-norm of the sequence $\{a_n\}$. It is this feature of the classic theorem that motivated our desire for improving the following, which is quoted from P. X. Gallagher [6].

Theorem 3. *Let $\cdot$ denote the usual dot product in $\mathbb{R}^n$ and $c(a)$ be a complex-valued function on $\mathbb{Z}^n$. Then*

$$\sum_{\substack{\beta\in\mathbb{R}^n/\mathbb{Z}^n\\ \mathrm{ord}(\beta)\le X}}\left|\sum_{\substack{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}^n\\ \max_{1\le i\le n}|\alpha_i|\le N}}c(\alpha)e(\alpha\cdot\beta)\right|^2\ll\left(N^n+X^{2n}\right)\sum_{\substack{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}^n\\ \max_{1\le i\le n}|\alpha_i|\le N}}|c(\alpha)|^2, \tag{1.5}$$

where the implied constant depends on n.

Here and after, $\mathrm{ord}(\beta)$ denotes the additive order of β in $\mathbb{R}^n/\mathbb{Z}^n$. Hence if $\beta=\left(\frac{a_1}{q_1},\cdots,\frac{a_n}{q_n}\right)$, then $\mathrm{ord}(\beta)=\mathrm{lcm}(q_1,\cdots,q_n)$. (1.5) follows easily from (1.4). But the result of Theorem 2 is more general than that of Theorem 3, as the outer summation of (1.4) can be considerably longer than that of (1.5). Hence it is believed that X^{2n} on the right-hand side of (1.5) can replaced, as noted before, by X^{n+1}, the length of the outer summation(see Lemma 2), in spirit analogous to that of the classical large sieve inequality. In other words, the majorant in (1.5) might be replaced by

$$\left(N^n+X^{n+1}\right)\sum_{\substack{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}^n\\ \max_{1\le i\le n}|\alpha_i|\le N}}|c(\alpha)|^2. \tag{1.6}$$

It is clear that both terms above are necessary. Set $c(\alpha)=1$ for all α and $N=1$, we see that X^{n+1} is needed. Taking $X=1$ and $c(\alpha)=e(-\alpha\cdot\beta)$ gives the conclusion that N^n is necessary. However, (1.6) is not enough. The following is a counter example. Let

$$T=\{\beta\in\mathbb{R}^n/\mathbb{Z}^n\ :\ \mathrm{ord}(\beta)\le X,\beta=(\beta_1,\cdots,\beta_n),\ \beta_i=0\text{ for }2\le i\le n,\ \beta=\frac{a_1}{q_1},\ q_1\in\mathbb{P}\},$$

where $\mathbb{P}$ denotes the set of prime numbers. It is clear that T is of size $\gg X^{2-\epsilon}$, as it can be identified with the Farey fractions of level X with prime denominators. Let $c(\alpha) = 1$ for all α. We have

$$\begin{aligned}
& \sum_{\substack{\beta\in\mathbb{R}^n/\mathbb{Z}^n \\ \mathrm{ord}(\beta)\le X}} \left| \sum_{\substack{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}^n \\ \max_{1\le i\le n}|\alpha_i|\le N}} c(\alpha) e(\alpha\cdot\beta) \right|^2 \\
\ge & \sum_{\beta\in T} \left| \sum_{\substack{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}^n \\ \max_{1\le i\le n}|\alpha_i|\le N}} c(\alpha) e(\alpha\cdot\beta) \right|^2 \\
= & N^{2n-2} \sum_{\substack{1\le p\le X \\ p\in\mathbb{P}}} \sum_{\substack{a \bmod p \\ \gcd(a,p)=1}} \left| \sum_{|m|\le N} e\left(\frac{a}{q}m\right) \right|^2 \\
= & N^{2n-2} \sum_m \sum_{m'} \sum_{\substack{1\le p\le X \\ p\in\mathbb{P}}} \sum_{\substack{a \bmod p \\ \gcd(a,p)=1}} e\left(\frac{a}{p}(m-m')\right) \\
= & N^{2n-2} \left[\sum_m \sum_{m'} \sum_{\substack{1\le p\le X \\ p\in\mathbb{P} \\ p|(m-m')}} (p-1) - \sum_m \sum_{m'} \sum_{\substack{1\le p\le X \\ p\in\mathbb{P} \\ p\nmid(m-m')}} 1 \right] \\
= & N^{2n-2} \left[\sum_{\substack{1\le p\le X \\ p\in\mathbb{P}}} \sum_m \sum_{\substack{m' \\ p|(m-m')}} p - \sum_{\substack{1\le p\le X \\ p\in\mathbb{P}}} \sum_m \sum_{m'} 1 \right] \\
\ge & c(\epsilon) N^{2n-1} X^{2-\epsilon} - \pi(X) N^{2n}, \qquad (1.7)
\end{aligned}$$

for some $c(\epsilon) > 0$ that depends only on ϵ and as usual $\pi(x)$ denotes the number of primes not exceeding x. But (1.6) gives the majorant of

$$N^{2n} + N^n X^{n+1}.$$

Taking $N = X^{1+\theta}$ for any $0 < \theta < 1$, which ensures the dominance of the positive term in (1.7), we see that the majorant of (1.6) is not enough.

The following notations and conventions are used throughout paper.

$e(z) = \exp(2\pi i z) = e^{2\pi i z}$.
$f = O(g)$ means $|f| \le cg$ for some unspecified postive constant c.
$f \ll g$ means $f = O(g)$.
$f \asymp g$ means $f \ll g$ and $g \ll f$. Unless otherwise stated, all implied constants in $\ll$, O and $\asymp$ are absolute.
$\square$ denotes the end of a proof or the proof is easy and standard.

Acknowledgment. The author wishes to thank Professors P. X. Gallagher and J. B. Friedlander, the former for suggesting the problem and both for the helpful discussions. The author was supported by a grant from the Faculty Development and Research Fund at the United States Military Academy and a post-doctoral fellowship at the University of Toronto during this work.

2. Preliminary Lemmas

In this section, we quote the lemmas needed for the results of this paper. As in the best-known proof of the classical large sieve inequality, we need the duality principle.

Lemma 1 (Duality Principle)**.** *Let $T = [t_{mn}]$ be a square matrix with entries from the complex numbers. The following two statements are equivalent:*

(1) *For any absolutely square summable sequence of complex numbers $\{a_n\}$, we have*

$$\sum_m \left| \sum_n a_n t_{mn} \right|^2 \leq D \sum_n |a_n|^2. \tag{2.1}$$

(2) *For any absolutely square summable sequence of complex numbers $\{b_n\}$, we have*

$$\sum_n \left| \sum_m b_m t_{mn} \right|^2 \leq D \sum_m |b_m|^2. \tag{2.2}$$

Proof. This is a standard result. See Theorem 288 in [7]. □

We shall also need the following lemma regarding the spacing of certain n dimensional vectors. Here and after, we set

$$S = \left\{ \beta \in \mathbb{R}^n/\mathbb{Z}^n : \mathrm{ord}(\beta) \leq X,\ \beta = \left(\frac{a_1}{q_1},\ \cdots\ \frac{a_n}{q_n} \right),\ \frac{X}{2} \leq q_1 \leq X \right\}.$$

Lemma 2. *Let $\epsilon > 0$ be given and $Y > 0$*

$$M(X,Y) = \max_{\beta \in S} \# \left\{ \beta' \in S\ :\ \|\beta - \beta'\| < Y \right\}.$$

Then we have

$$M(X,Y) \ll X^{\epsilon} \left(X^{n+1} Y^n + X^2 Y + 1 \right), \tag{2.3}$$

where the implied constant depends on n and ϵ.

Proof. We estimate the size of the set of our interest in the following way. Fix $\beta = \left(\frac{a_1}{q_1}, \cdots, \frac{a_n}{q_n} \right) \in S$. The number of $\frac{a_1'}{q_1'}$'s with $1 \leq a_1' < q_1'$, $X/2 < q_1' \leq X$ and $\gcd(a_1', q_1') = 1$ such that $\left\| \frac{a_1}{q_1} - \frac{a_1'}{q_1'} \right\| < Y$ does not exceed $X^2 Y + 1$. For each such $\frac{a_1'}{q_1'}$, we have the following number of choices for the other coordinates of β'.

$$\sum_{i=1}^{[X/q_1']+1} \left(\sum_{k | i q_1'} (kY+1) \right)^{n-1} \ll \sum_{i=1}^{[X/q_1']+1} \left(Y^{n-1} (i q_1')^{n-1+\epsilon} + (i q_1')^{\epsilon} \right) \ll Y^{n-1} X^{n-1+\epsilon} + X^{\epsilon}.$$

Recall that $X/2 \leq q_1' \leq X$. Hence in total, we have

$$M(X,Y) \ll Y^n X^{n+1+\epsilon} + Y^{n-1} X^{n+\epsilon} + Y X^{2+\epsilon} + X^{\epsilon}.$$

The term $Y^{n-1} X^{n+\epsilon}$ is not necessary, for $Y^{n-1} X^{n+\epsilon} \geq Y X^{2+\epsilon}$ implies $XY \geq 1$ and hence $Y^{n-1} X^{n+\epsilon} \leq Y^n X^{n+1+\epsilon}$. Hence the result follows. □

Note that upon taking $Y = 1$, we get the the size of the set S is $O_{\epsilon}(X^{n+1+\epsilon})$. Therefore, in the light of Lemma 2, so long as Y is not so small that no regularity of distribution of elements of S can be expected, the spacing property of S is essentially as expected, as given in the first term of (2.3).

It is somewhat a melancholy admission, as will be noted in Section 4, that the term $X^{2+\epsilon} Y$ is necessary in Lemma 2. The following is an example to that effect. Let

$$T' = \{ \beta \in \mathbb{R}^n/\mathbb{Z}^n\ :\ \mathrm{ord}(\beta) \leq X, \beta = (\beta_1, \cdots, \beta_n),\ \beta_i = 0 \text{ for } 2 \leq i \leq n \},$$

The spacing properties of elements in T' are the same as those of the Farey fractions of level X. Hence

$$\max_{\beta\in T'} \#\left\{\beta'\in T' \,:\, \|\beta-\beta'\|<Y\right\} \asymp X^2Y+1.$$

Therefore, we have $M(X,Y)\gg X^2Y$. Taking $Y=X^{-1-\theta}$ for any $0<\theta<1$, we see that the term X^2Y is needed in (2.3).

3. Main Contention

The objective is to have an upper bound for the following sum.

$$\sum_{\substack{\beta\in\mathbb{R}^n/\mathbb{Z}^n\\ \mathrm{ord}(\beta)\le X}} \left| \sum_{\substack{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}^n\\ \max_{1\le i\le n}|\alpha_i|\le N}} c(\alpha)e(\alpha\cdot\beta)\right|^2.$$

Without trying too hard and in the light of Lemma 2, simply applying Cauchy's inequality would give us the majorant of

$$N^nX^{n+1+\epsilon}\sum_{\alpha}|c(\alpha)|^2,$$

which is already better than (1.5) when $N^n\ll X^{n-1-\epsilon}$. But certainly we hope to do better than *this*. Furthermore, some applications require that the size of X is well controlled. To that end, we have the following.

Theorem 4. *Under the notations that have been in use thus far, we have*

$$\sum_{\substack{\beta\in\mathbb{R}^n/\mathbb{Z}^n\\ \mathrm{ord}(\beta)\le X}} \left| \sum_{\substack{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}^n\\ \max_{1\le i\le n}|\alpha_i|\le N}} c(\alpha)e(\alpha\cdot\beta)\right|^2 \ll X^\epsilon\left(X^{n+1}+N^{n-1}X^2+N^n\right)\sum_{\alpha}|c(\alpha)|^2, \tag{3.1}$$

where the implied constant depends on n and ϵ.

Proof. It will suffice to break up the outer sums into dyadic intervals. Together with the application of the duality principle, Lemma 1, it suffices to show that

$$\sum_{\alpha}\left|\sum_{\beta\in S} b(\beta)e(\alpha\cdot\beta)\right|^2 \ll X^\epsilon\left(X^{n+1}+N^{n-1}X^2+N^n\right)\sum_{\beta}|b(\beta)|^2, \tag{3.2}$$

for any sequence of complex numbers $\{b(\beta)\}$ and where S and the summations over α and β are as before.

Set $\phi(x)=\left(\dfrac{\sin\pi x}{2x}\right)^2$. By positivity, the left-hand side of (3.2) is bounded above by

$$\sum_{\alpha\in\mathbb{Z}^n}\prod_{i=1}^n\phi\left(\frac{\alpha_i}{2N}\right)\left|\sum_{\beta\in S} b(\beta)e(\alpha\cdot\beta)\right|^2,$$

where the sum over α is now extended over all elements of $\mathbb{Z}^n$. Expanding the modulus square in the above and factoring, it becomes

$$\begin{aligned}&\sum_{\beta\in S}\sum_{\beta'\in S} b(\beta)\bar{b}(\beta')\sum_{\alpha\in\mathbb{Z}^n}\prod_{i=1}^n\phi\left(\frac{\alpha_i}{2N}\right)e(\alpha_i(\beta_i-\beta_i'))\\ &= \sum_{\beta\in S}\sum_{\beta'\in S} b(\beta)\bar{b}(\beta')\prod_{i=1}^n\sum_{\alpha_i=-\infty}^{\infty}\phi\left(\frac{\alpha_i}{2N}\right)e(\alpha_i(\beta_i-\beta_i'))\end{aligned} \tag{3.3}$$

Set $V(y) = \sum_{n=-\infty}^{\infty} \phi\left(\frac{n}{2N}\right) e(ny)$. Recall that the Fourier transform of $\phi(x)$ is precisely $\Lambda(s) = \max(1-|s|, 0)$. Hence, we apply the Poisson summation formula and a change of variables to obtain

$$\begin{aligned} V(y) &= 2N \sum_{m=-\infty}^{\infty} \Lambda(2N(m+y)) \\ &= \frac{\pi^2 N}{2} \sum_{|m+y|<(2N)^{-1}} (1-2N|m+y|) \\ &= \frac{\pi^2 N}{2}(1-2N\|y\|), \end{aligned}$$

if $\|y\| < (2N)^{-1}$ and $V(y) = 0$ otherwise. Therefore, (3.3) is

$$\begin{aligned} &= \left(\frac{\pi^2 N}{2}\right)^n \sum_{\substack{\beta \\ \|\beta-\beta'\|<(2N)^{-1}}} \sum_{\beta'} b(\beta)\bar{b}(\beta') \prod_{i=1}^{n} (1-2N\|\beta_i - \beta_i'\|) \\ &\leq \left(\frac{\pi^2 N}{2}\right)^n \sum_{\substack{\beta \\ \|\beta-\beta'\|<(2N)^{-1}}} \sum_{\beta'} |b(\beta)\bar{b}(\beta')| \\ &\leq \left(\frac{\pi^2 N}{2}\right)^n \sum_{\beta} |b(\beta)|^2 M(X, (2N)^{-1}), \end{aligned}$$

with $M(X, Y)$ defined as in Lemma 2. Upon inserting the result of Lemma 2 with $Y = (2N)^{-1}$ and summing up all the dyadic intervals for X, our contention follows. □

From the discussion and the examples given in section 1, we can infer that the inequality in (3.1) is essentially the best possible.

4. Notes

It was the inequality (1.5) that was the starting point for P. X. Gallagher [6] in improving an estimate on the number $E_n(N)$ of monic polynomials

$$F(x) = X^n + a_1 X^{n-1} + \cdots + a_n$$

with integer coefficients and of height, $H(F) = \max(|a_1|, \cdots, |a_n|)$ not exceeding N for which the Galois group is a proper subgroup of the symmetric group. The problem was first studied by van der Waerden [15] and improvements were later made by Knobloch [9, 10]. Gallagher's improvement gives the bound

$$E_n(N) \ll N^{n-\frac{1}{2}} \log N,$$

with the implied constant depending on n. The size of X required to ensure the dominance of N^n in (1.5) is the key factor for determining the negative part of the exponent of N above. Unfortunately, our result (3.1) requires the exact same size for X to ensure the dominance of N^n and hence it leads to essentially the same bounds for $E_n(N)$ as above.

References

[1] M. B. Barban, *The "large sieve" method and its applications in the theory of numbers*, Uspehi Matematiks Nauk **21** (1966), 51–102.

[2] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Société Mathematics France **18** (1974).

[3] E. Bombieri and H. Davenport, *Some inequalities involving trigonometrical polynomials*, Annali Scuola Normale Superiore - Pisa **23** (1969), 223–241.

[4] H. Davenport and H. Halberstam, *The values of a trigonometric polynomial at well spaced points*, Mathematika **13** (1966), 91–96, *Corrigendum and Addendum*, Mathematika **14** (1967), 232-299.

[5] P. X. Gallagher, *The large sieve*, Mathematika **14** (1967), 14–20.

[6] ———, *The large sieve and probabilistic Galois theory*, Proceedings of Symposium on Pure Mathematics, vol. XXIV, American Mathematical Society, 1973, pp. 91–101.
[7] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, Cambridge University Press, 1964.
[8] M. N. Huxley, *The large sieve inequality for algebraic number fields*, Mathematika **15** (1968), 178–187.
[9] H.-W. Knobloch, *Zum hilbertschen irreduzibilitätssatz*, Abh. Math. Sem. Univ. Hamburg. **19** (1955), 176–190.
[10] ———, *Die seltenheit der reduziblen polynome*, Jber. Deutsch. Math. Verein **59** (1956), 12–19.
[11] J. V. Linnik, *The large sieve*, Doklady Akademii Nauk Soiuza Sovetskikh Sotsialisticheskikh Respublik **36** (1941), 119–120, (Russian).
[12] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics, vol. 227, Spring-Verlag, Barcelona, etc., 1971.
[13] ———, *The Analytic Priciples of Large Sieve*, Bulletin of the American Mathematical Society **84** (1978July), 547–567.
[14] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.
[15] B. L. van der Waerden, *Die seltenheit der gleichungen mit affekt*, Math. Ann. **109** (1934), 13–16.
[16] L. Zhao, *Large sieve inequality for characters to square moduli*, Acta Arithmetica **112** (2004), 297–308.
[17] ———, *Large sieve inequality for special characters to prime square moduli*, Functiones et Approximatio Commentarii Mathematici **XXXII** (2004), 1–8.

Department of Mathematics
University of Toronto
100 Saint George Street
Toronto, ON M5S 3G3 Canada
Email Address: lzhao@math.toronto.edu